GOVERNMENT OF INDIA
FINANCE
LOK SABHA

UNSTARRED QUESTION NO:823
ANSWERED ON:17.08.2007
INTRODUCTION OF E-STAMPS
Fanthome Shri Francis

Will the Minister of FINANCE be pleased to state:

(a) whether the Government is considering a proposal to introduce e-stamps to register public documents;

(b) if so, the details thereof;

(c) the precautions taken to ensure that there are no counterfeit e-stamps used;

(d) whether the Stock Holding Corporation of India has approved the proposal to use e-stamps; and

(e) if so, the details thereof?

Answer

MINISTER OF STATE IN THE MINISTRY OF FINANCE (SHRI P.K.BANSAL)

(a) to (e) : Government has already decided to implement e-stamping system on a pilot basis in some selected cities in India, and has authorised the Stock Holding Corporation of India Limited(SHCIL) to function as Central Record Keeping Agency for the project. SHCIL is providing the e-stamping system to the States desirous to participate in the project. The system has become operational in February 2007 in two cities in Gujarat namely, Ahmedabad and Gandhinagar and is functioning smoothly. The e-stamps contain following hi-tech security features to prevent counterfeiting:-

(i) Unique Identification Number (UIN) - The stamp certificate is generated by the system with a Unique Identification Number (UIN), which is not repeated. Anyone can verify the stamp certificate on the e-stamping website with the UIN.

(ii) 2D bar coding - encrypting the important identification content of the stamp certificate to ensure tamper-proof certificate.

(iii) Optical watermarking - to eliminate the possibility of duplication of the stamp certificate. The advantage is when a photocopy of the certificate is made, the watermark on the document will change to a text as `Copy`.

(iv) Microprint - Micro printing works as anti-counterfeiting feature through the fact that text of such small size is very difficult to reproduce.

(v) The access to the e-stamping system is given to authorized users, who are given user I.D. and initial password. The user is required to change the initial password and then is authorized to access the system. The user needs to change the passwords on a regular basis.